Notice of Allowability	Application No.	Applicant(s)	
	09/830,180	BILCHEV, GEORGE	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *11/22/2005*.

2. ☒ The allowed claim(s) is/are *1-70 and 79-83*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☒ Other ~~Text~~ page dated 4/23/01

DETAILED ACTION

Applicant's arguments submitted on 11/22/2005 were considered and were persuasive. The finality of the previous office action is hereby withdrawn. Claims 1-83 were examined.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Larry Nixon on 12/19/2005. The application has been amended as follows:

IN THE SPECIFICATION:

Insert the following text above line 2 on page 1 (see attached insert as example):

This application is a national state entry of PCT/GB99/03891 filed 11/23/1999, which claims priority from British application 9825644.9 filed 11/23/1998.

IN THE CLAIMS:

A consolidated listing of all the claims is listed below. The claims that have been amended via examiner's amendments are noted in parenthesis as "examiner's amendment". The claims previously amended by applicant are noted as "previously

amended". Original claims are noted as "original". Claims 71-78 are cancelled with applicant's permission and are noted as cancelled below.

Claim 1 (examiner's amendment):

Encipher apparatus for enciphering a signal, comprising:

forming means for receiving the signal to be enciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

a plurality of encipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means; and

configuring means,

wherein each encipher functional module comprises

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and lo produce at its corresponding parallel output a corresponding enciphered set of bits;

and each encipher functional module is operable under the control of the configuring means to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an enciphered data block in which said respective

predetermined set of bits is replaced by the corresponding enciphered set of bits produced at the parallel output of its data processing unit.

Claim 2 (original):

Encipher apparatus according to claim 1, wherein said respective data processing units are of a single type.

Claim 3 (previously amended):

Encipher apparatus according to claim 1, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the set of bits received at its parallel input.

Claim 4 (previously amended):

Encipher apparatus according to claim 1 wherein each of said data processing units is a reversible gate.

Claim 5 (original):

Encipher apparatus according to claim 3, wherein said reversible gate comprises a Fredkin's gate or an AND/NAND gate.

Claim 6 (previously amended):

Encipher apparatus according to claim 1 wherein said configuring means is operative to control said encipher functional modules in accordance with a cipher design description.

Claim 7 (original):

Encipher apparatus according to claim 6, including means for receiving said cipher design description.

Claim 8 (original):

Encipher apparatus according to claim 6, including means for generating said cipher design description.

Claim 9 (original):

Encipher apparatus according to claim 8, wherein the generating means includes a random or pseudo-random number generator and is operative to use random or pseudo-random numbers generated by said random or pseudo-random number generator to describe in code said respective predetermined sets of bits.

Claim 10 (examiner's amendment):

Encipher apparatus according to claim 1, wherein each of said plurality of encipher functional modules comprises a logic gate which does not conserve logic.

Claim 11 (previously amended):

Encipher apparatus according to claim 1, wherein said plurality of encipher functional modules form a programmable circuit.

Claim 12 (original):

Encipher apparatus according to claim 11, wherein said plurality of encipher functional modules comprises a programmable logic gate array, and said configuring means comprises a programming means for programming said programmable logic gate array.

Claim 13 (original):

Encipher apparatus according to claim 11, wherein each of said plurality of encipher functional modules comprises analogue electronic modules.

Claim 14 (examiner's amendment):

Encipher apparatus according to claim 1, wherein the signal is an optical signal and each of said plurality of encipher functional modules comprises optical components.

Claim 15 (examiner's amendment):

Encipher apparatus according to claim 1, comprising a programmable computing apparatus, wherein each of said plurality of encipher functional modules comprises a computer code routine implemented on said programmable computing apparatus.

Claim 16 (original):

Encipher apparatus according to claim 15, wherein said computer code routine is in the form of a generic module code routine repeatedly implemented dependent upon information from said configuring means.

Claim 17 (previously amended):

Encipher apparatus according to claim 1 including first selection means for selecting a type of encipher functional module to be used from amongst a plurality of possible types of encipher functional modules, wherein said configuring means is adapted to configure the encipher apparatus to use the selected type of encipher functional module.

Claim 18 (examiner's amendment):

Encipher apparatus according to claim 1, including second selection means for selecting the number of said plurality of encipher functional modules to be used, wherein said configuring means is adapted to configure the encipher apparatus to use the selected number of encipher functional modules.

Claim 19 (examiner's amendment):

Encipher apparatus according to claim 1, including third selection means for selecting for each of said plurality of encipher functional modules the respective predetermined set of the bits of a data block received at its module input.

Claim 20 (examiner's amendment):

A method of enciphering a signal, the method comprising:

receiving the signal to be enciphered and forming the signal into a sequence of data blocks, each having a first predetermined number of bits;

applying the sequence of data blocks to a plurality of encipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks,

each encipher functional module comprising

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits; and

configuring each encipher functional module to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output an enciphered data block in which said respective predetermined set of bits is replaced by the corresponding enciphered set of bits produced at the parallel output of its data processing unit.

Claim 21 (original):

A method according to claim 20, wherein the encipher functional modules are of a single type.

Claim 22 (previously amended):

A method according to claim 20, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input.

Claim 23 (examiner's amendment):

A method according to claim 20, wherein each of said plurality of encipher functional modules each act as a reversible gate.

Claim 24 (examiner's amendment):

A method according to claim 20, wherein the configuring of each of said encipher functional modules is in accordance with a cipher design description.

Claim 25 (original):

A method according to claim 24, including receiving said cipher design description.

Claim 26 (original):

A method according to claim 24, including generating said cipher design description.

Claim 27 (original):

A method according to claim 24, including generating random or pseudo-random numbers and using the generated random or pseudo-random numbers to generate said cipher design description.

Claim 28 (examiner's amendment):

A method according to claim 27, wherein a respective generated random or pseudo-random number is used to describe in code the respective predetermined set of bits for a respective encipher functional module.

Claim 29 (original):

A method according to claim 28, wherein the logic operations do not conserve logic.

Claim 30 (examiner's amendment):

A method according to claim 20, wherein each of said plurality of encipher functional modules comprises a programmable logic gate array and the configuring step includes programming said programmable logic gate array.

Claim 31 (examiner's amendment):

A method according to claim 20, implemented by computer code on a computing apparatus, wherein each of said plurality of encipher functional modules comprises a computer code routing implemented in dependence upon configuration information.

Claim 32 (examiner's amendment):

A method according to claim 31, wherein the computer code routine is implemented repeatedly dependent upon the number of encipher functional modules to be implemented.

Claim 33 (previously amended):

A method according to claim 20, including selecting the type of encipher functional module to be used from amongst a plurality of possible types of encipher functional modules.

Claim 34 (examiner's amendment):

A method according to claim 20, including selecting the number of each of said plurality of encipher functional modules used.

Claim 35 (examiner's amendment):

A method according to claim 20, including selecting the respective predetermined set of the bits of a received data block for each of said plurality of encipher functional modules.

Claim 36 (examiner's amendment):

Decipher apparatus for deciphering a signal, comprising:

forming means for receiving the signal to be deciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means; and

configuring means,

wherein each decipher functional module comprises

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits;

and each decipher functional module is operable under the control of the configuring means to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit.

Claim 37 (examiner's amended):

Decipher apparatus according to claim 36, wherein said decipher functional modules are of a single type.

Claim 38 (examiner's amendment):

Decipher apparatus according to claim 36, wherein said configuring means is operative to control each of said plurality of decipher functional modules in accordance with a cipher design description.

Claim 39 (original):

Decipher apparatus according to claim 38, wherein cipher design description is equivalent to the inverse of a cipher design description used to control encipher functional modules of an encipher apparatus used to produce the enciphered signal.

Claim 40 (previously amended):

Decipher apparatus according to claim 38, including means for receiving said cipher design description.

Claim 41 (previously amended):

Decipher apparatus according to claim 38, including means for generating said cipher design description.

Claim 42 (original):

Decipher apparatus according to claim 41, wherein the generating means includes a random or pseudo-random number generator and is operative to use random or pseudo-random numbers generated by said random or pseudo-random number generator to describe in code said respective predetermined sets of bits.

Claim 43 (previously amended):

Decipher apparatus according to claim 36, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input.

Claim 44 (previously amended):

Decipher apparatus according to claim 36, wherein each of said data processing units comprises a reversible gate.

Claim 45 (original):

Decipher apparatus according to claim 44, wherein said reversible gate comprises a Fredkin's gate or an AND/NAND gate.

Claim 46 (examiner's amendment):

Decipher apparatus according to claim 36, wherein each of said plurality of decipher functional modules comprises a logic gate which does not conserve logic.

Claim 47 (examiner's amendment):

Decipher apparatus according to claim 36, wherein each of said plurality of decipher functional modules form a programmable circuit.

Claim 48 (original):

Decipher apparatus according to claim 47, wherein said plurality of decipher functional modules comprise a programmable logic gate array, and said configuring means comprises a programming means for programming said programmable logic gate array.

Claim 49 (examiner's amendment):

Decipher apparatus according to claim 36, wherein the signal is an optical signal and each of said plurality of decipher functional modules comprises optical components.

Claim 50 (examiner's amendment):

Decipher apparatus according to claim 36, comprising a programmable computing apparatus, wherein each of said plurality of decipher functional modules comprise a computer code routine implemented on said programmable computing apparatus.

Claim 51 (examiner's amendment):

Decipher apparatus according to claim 50, wherein each of said plurality of decipher functional modules comprise a computer code routing repeatedly implemented upon information from said configuring means.

Claim 52 (examiner's amendment):

Decipher apparatus according to claim 36, wherein said configuring means is responsive to type identifying information included in a cipher design description to

configure the type of each of said plurality of decipher functional modules in accordance with said type identifying information.

Claim 53 (examiner's amendment):

Decipher apparatus according to claim 36, wherein said configuring means is responsive to module number information included in a cipher design description to configure a corresponding number of each of said plurality of decipher functional modules.

Claim 54 (examiner's amendment):

Decipher apparatus according to claim 36, wherein said configuring means is responsive to data block size information included in a cipher design description adapted to configure the input and output of each of said plurality of decipher functional modules.

Claim 55 (examiner's amendment):

A method of deciphering an enciphered signal, the method comprising:

receiving the signal to be deciphered and outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

applying the sequence of data blocks to a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks,

each decipher functional module comprising

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits; and

configuring each decipher functional module to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit.

Claim 56 (original):

A method according to claim 55, wherein the decipher functional modules are of a single type.

Claim 57 (previously amended):

A method according to claim 55, wherein the reversible process of at least one of said data processing units is a switching operation controlled by at least one of the bits of a data block received at its parallel input.

Claim 58 (examiner's amendment):

A method according to claim 55, wherein each of said plurality of decipher functional modules act as a reversible gate.

Claim 59 (examiner's amendment):

A method according to claim 55, wherein the configuring of each of said plurality of decipher functional modules is in accordance with a cipher design description.

Claim 60 (original):

A method according to claim 59, including receiving said cipher design description.

Claim 61 (original):

A method according to claim 59, including generating said cipher design description.

Claim 62 (original):

A method according to claim 59, including generating random or pseudo-random numbers and using the generated random or pseudo-random numbers to generate said cipher design description.

Claim 63 (original):

A method according to claim 62, wherein a respective generated random or pseudo-random number is used to describe in code the respective predetermined set of bits for a respective decipher functional module.

Claim 64 (original):

A method according to claim 63, wherein the logic operations do not conserve logic.

Claim 65 (examiner's amendment):

A method according to claim 55, wherein each of said plurality of decipher functional modules comprises a programmable logic gate array and the configuring step includes programming said programmable logic gate array.

Claim 66 (examiner's amendment):

A method according to claim 55, implemented by computer code on a computing apparatus, wherein each of said plurality of decipher functional modules comprises a computer code routine implemented in dependence upon configuration information.

Claim 67 (original):

A method according to claim 66, wherein the computer code routine is implemented repeatedly dependent upon the number of said decipher functional modules to be implemented.

Claim 68 (previously amended):

A method according to claim 55, including selecting the type of decipher functional module to be used from amongst a plurality of possible types of decipher functional modules.

Claim 69 (examiner's amendment):

A method according to claim 55, including selecting the number of each of said plurality of decipher functional modules used.

Claim 70 (examiner's amendment):

A method according to claim 55, including selecting the respective predetermined set of bits of a received data block for each of said plurality of decipher functional modules.

Claims 71-78 (cancelled).

Claim 79 (examiner's amendment):

Cipher apparatus comprising the encipher apparatus of claim 1 and a decipher apparatus for deciphering a signal comprising:

forming means for receiving the signal to be deciphered and for outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks from the forming means; and

configuring means,

wherein each decipher functional module comprises

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits, and is operable under the control of the configuring means of the decipher apparatus to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit;

wherein each of said plurality of said encipher functional modules of the encipher apparatus are constituted by each of said plurality of decipher functional modules of the decipher apparatus but are sequentially coupled in the opposite order.

Claim 80 (examiner's amendment):

A cipher method for enciphering and deciphering a signal comprising the encipher method of claim 20 and a decipher method comprising:

receiving the signal to be deciphered and outputting the signal as a sequence of data blocks, each having a first predetermined number of bits;

applying the sequence of data blocks to a plurality of decipher functional modules sequentially coupled to operate sequentially on the sequence of data blocks, each of said plurality of said decipher functional module comprising:

a module input,

a module output, and

a respective data processing unit having a parallel input and a corresponding parallel output and being arranged to perform a respective reversible process upon a set of bits at its parallel input and to produce at its corresponding parallel output a corresponding enciphered set of bits; and

configuring each of said plurality of decipher functional modules to couple a respective predetermined set of the bits of a data block received at its module input to the parallel input of its data processing unit and to provide at its module output a deciphered data block in which said respective predetermined set of bits is replaced by the corresponding deciphered set of bits produced at the parallel output of its data processing unit.

Claim 81 (examiner's amendment):

Processor implemented instructions stored on a computer readable storage medium, the processor implemented instructions causing a processor to carry out the method of claim 20.

Claim 82 (original):

A carrier medium carrying the processor implemented instructions according to claim 81.

Claim 83 (previously amendment):

A storage medium storing logic to configure a programmable logic gate array to carry out the method of claim 20.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

PP